

An das
Bundesministerium für Justiz

**Betrifft: Entwurf eines Bundesgesetzes, mit dem das Strafgesetzbuch, das Strafvollzugsgesetz, das Jugendgerichtsgesetz 1988 und das Strafregistergesetz geändert werden
Stellungnahme des Datenschutzrates**

Der **Datenschutzrat** hat in seiner 191. Sitzung am 16. November 2009 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

Zu § 15c Strafvollzugsgesetz (StVG):

§ 15c StVG räumt der Bundesministerin für Justiz, dem Leiter der Vollzugsdirektion, dem Anstaltsleiter sowie bestimmten Bediensteten auch nach Ablauf von zehn Jahren ab dem Zeitpunkt, zu dem die letzte Haft oder Unterbringung beendet wurde, noch einen Zugriff auf Daten von ehemaligen Strafgefangenen ein.

Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung gemäß § 1 Abs. 2 DSG 2000 nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Eine Verwendung von personenbezogenen Daten darf sohin im Sinne des Verhältnismäßigkeitsgrundsatzes (gemäß § 1 Abs. 2 DSG 2000) nur solange

erfolgen, als überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. Es kann jedoch in keiner Weise nachvollzogen werden, zu welchem Zweck die in § 15c Abs. 1 genannten Personen auch noch nach Ablauf von zehn Jahren ab dem Zeitpunkt, zu dem die letzte Haft oder Unterbringung beendet wurde, noch einen Zugriff auf Daten von ehemaligen Strafgefangenen ein erhalten sollen. Nachdem in diesem Fall kein überwiegendes berechtigtes Interesse des Auftraggebers oder eines Dritten die Verwendung die Daten nach Ablauf von zehn Jahren erfordern, darf auch den in § 15c Abs. 1 genannten Personen nach Ablauf von zehn Jahren ab dem Zeitpunkt, zu dem die letzte Haft oder Unterbringung beendet wurde, keine Zugriffsrecht auf diese Daten mehr eingeräumt werden.

Darüber hinaus ist auch nicht einmal erkennbar, welche (allenfalls sogar sensible) Daten des ehemaligen Strafgefangenen vom Zugriff erfasst sind. In diesem Zusammenhang wird angemerkt, dass auch „strafrechtlich relevante“ Daten von der Europaratskonvention 108 und der RL 95/46/EG in die Nähe der sensiblen Daten gerückt werden.) Weiters sollte für die in Abs. 1 leg. cit. genannten Personen eine zeitliche Beschränkung für den Zugriff auf Daten des ehemaligen Strafgefangenen festgelegt werden.

Gemäß § 15c Abs. 2 unterliegen die Daten nicht dem eingeschränkten Datenzugriff, sobald die betreffende Person neuerlich in einer Justizanstalt angehalten wird. Dazu ist zu bemerken, dass selbst in jenem Fall, in dem eine Personen neuerlich in einer Justizanstalt angehalten wird, die Daten dieser angehaltenen Person im Sinne des Verhältnismäßigkeitsgrundsatzes nur soweit verwendet werden dürfen, als überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. Insbesondere erscheint daher eine Einschränkung hinsichtlich der zugriffberechtigten Personen in Abs. 2 leg. cit. erforderlich.

Nicht dem eingeschränkten Datenzugriff unterliegen nach § 15c Abs. 3 die Daten Name, Vorname (Z 1 leg. cit.); Geburtsdatum, Geburtsort (Z 2 leg. cit.) sowie Vornamen der Eltern und Alias-Namen sowie weitere Daten, wenn sie zur eindeutigen Identifizierung bei der Aufnahme dienen (Z 3 leg. cit.).

Es sollte in § 15c Abs. 3 ergänzt werden, dass die dort genannten Daten im Falle der Aufnahme nicht dem eingeschränkten Datenzugriff unterliegen.

Weiters ist zu § 15c Abs. 3 anzumerken, dass der Wortlaut der Regelung („...nicht dem eingeschränkten Datenzugriff unterliegen...“) unklar formuliert ist. Nur aus den

Erläuterungen lässt sich erkennen, dass auf diese in Abs. 3 leg. cit. genannten Daten offenbar ein (zeitlich) unbeschränkter Datenzugriff vorgesehen ist. Dazu ist zu bemerken, dass die in den Erläuterungen angeführten Bewegungsgründe (wie zB das Wegfallen des Aufwandes für das Löschen der Daten) einen zeitlich unbeschränkten Datenzugriff keinesfalls zu rechtfertigen vermögen. Nachdem eine Verwendung von personenbezogenen Daten im Sinne des Verhältnismäßigkeitsgrundsatzes (gemäß § 1 Abs. 2 DSG 2000) nur solange erfolgen darf, als überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern, ist ein von vornherein zeitlich unbeschränkter Datenzugriff jedenfalls unzulässig.

Zudem müsste festgelegt werden, welche Personen nach § 15c Abs. 3 zugriffsberechtigt sind.

Darüber hinaus erscheint es nicht verhältnismäßig, dass auch die Vornamen der Eltern einem unbeschränkten Datenzugriff unterliegen. Weiters müsste exakt konkretisiert werden, was unter den Daten, die zur eindeutigen Identifizierung bei der Aufnahme dienen, zu verstehen ist (zB Größe und Fingerabdruck). Auch wird darauf hingewiesen, dass die Alias-Namen – soweit diese überhaupt benötigt werden – statt in Abs. 3 Z 3 leg. cit. aus systematischen Gründen zu der Aufzählung der Namen in Abs. 3 Z 1 leg. cit. hinzugefügt werden sollten.

Der Datenschutzrat weist in diesem Zusammenhang auf die Regelungen des Gesundheitstelematikgesetzes zur Vertraulichkeit und Integrität von Daten hin. Es sollte auch im § 15c vorgesehen werden, dass zur inhaltlichen Verschlüsselung der Daten kryptographische Verfahren einzusetzen sind, die nach dem jeweiligen Stand der Technik mit wirtschaftlich vernünftigem Aufwand nicht kompromittiert werden können, und darüber hinaus elektronische Signaturen zum Signieren von Datensätzen zu verwenden sind, damit sichergestellt werden kann, dass die Daten nur auf dafür vorgesehene Einrichtungen eingesehen werden können.

18. November 2009
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt